Vulnerablility Asessment Scan Report on a Unix Server Using Nmap

IP Address: 192.168.1.52

Prepared by: Aliu A. Sanusi

Date: 27th February 2025

Table of Contents

Introduction

The results of a penetration testing scan conducted on a Unix computer with the IP address 192.168.1.52 are shown in this report. The Nmap tool was used for the assessment. Information regarding the target system's security was gathered using the program.

The goal of this scan is to identify open ports, services, security flaws, and other hazards that an attacker may take advantage of. This document includes the tool's comprehensive results, relevant screenshots, and conclusions.

Objective

Nmap (Network Mapper) was used to scan the Unix machine to detect open ports, running services, and vulnerabilities.

Nmap Scan Report

Scan Command Used

nmap -A -p- 192.168.1.52

This is a **powerful Nmap scan** that provides **detailed information** about a target machine (192.168.10.44). Here's what each flag does:

Breaking it Down:

1. **nmap** → Calls the **Nmap** tool, which is used for network scanning and security auditing.
2. **-A (Aggressive Scan)** → Enables multiple advanced features, including:
   - OS detection
   - Version detection
   - Script scanning
   - Traceroute
3. **-p- (Scan All Ports)** → Scans **all 65,535 TCP ports** instead of just the default 1,000.
4. **192.168.1.52** → The target IP address being scanned.

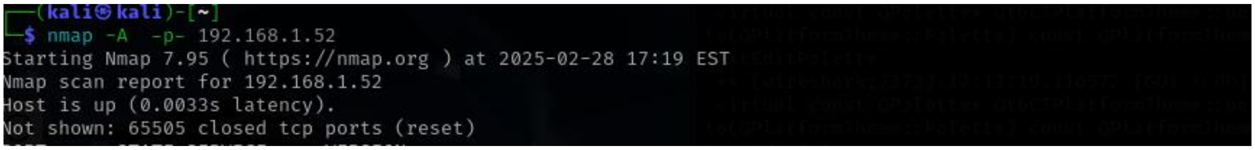
How It Helps in a Vulnerability Scan:

- **Identifies Open Ports** → Shows which services are running and where vulnerabilities might exist.
- **Detects Running Services & Versions** → Helps find outdated or misconfigured services.
- **Finds OS & System Info** → Useful for fingerprinting a system to tailor attacks or defenses.
- **Performs Traceroute** → Helps map out the network for possible attack paths.

Findings from Nmap Scan on 192.168.1.52

General Information:

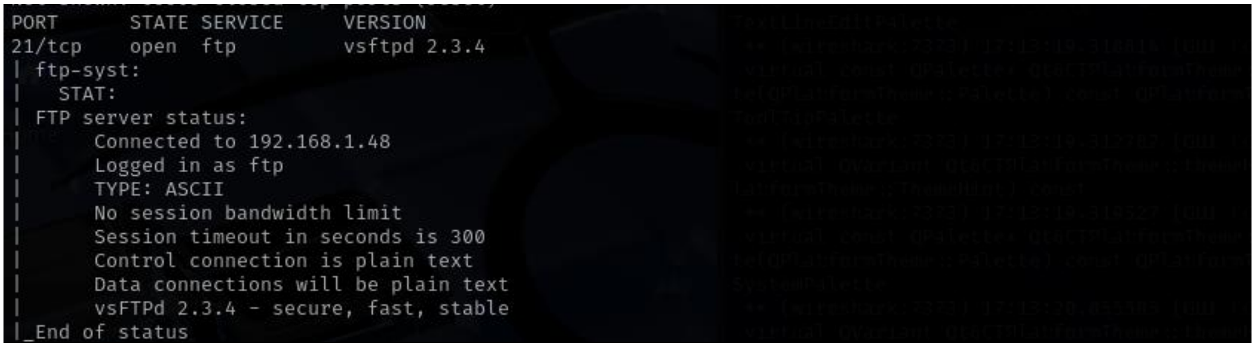
- **Target IP:** 192.168.1.52
- **Host is up:** 0.00033s latency
- **Operating System:** Linux 2.6.9 - 2.6.33
- **Network Distance:** 1 hop
- **MAC Address:** 08:00:27:6A:13:6E (Oracle VirtualBox virtual NIC)
- **Hostname:** metasploitable.localdomain



```
┌──(kali㉿kali)-[~]
└─$ nmap -A  -p- 192.168.1.52
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 17:19 EST
Nmap scan report for 192.168.1.52
Host is up (0.0033s latency).
Not shown: 65505 closed tcp ports (reset)
```

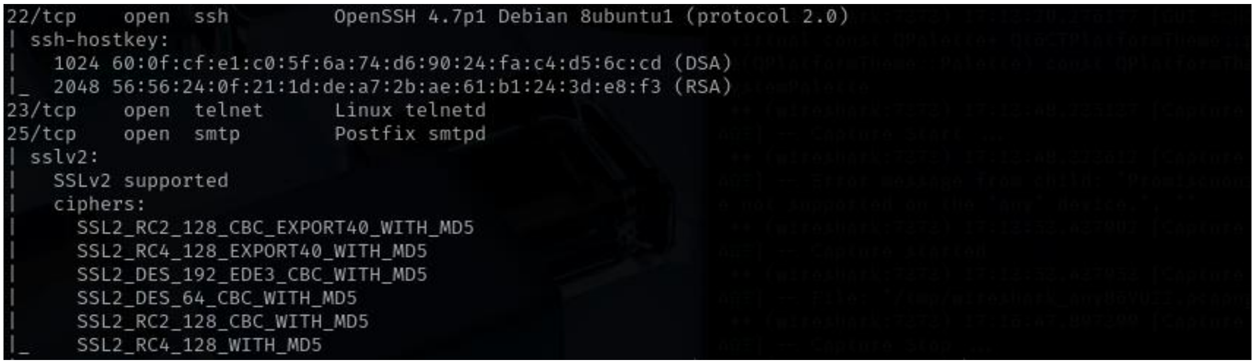
Open Ports and Services:

1. **FTP (Port 21)**
   - **Service:** vsftpd 2.3.4
   - **Anonymous Login:** Enabled
   - **Vulnerability:** This version is known to have a backdoor vulnerability (CVE-2011-2523).



```
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.48
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

2. **SSH (Port 22)**
   - **Service:** OpenSSH 4.7p1 Debian 8ubuntu1
   - **Vulnerability:** Outdated version, possibly vulnerable to multiple known exploits.

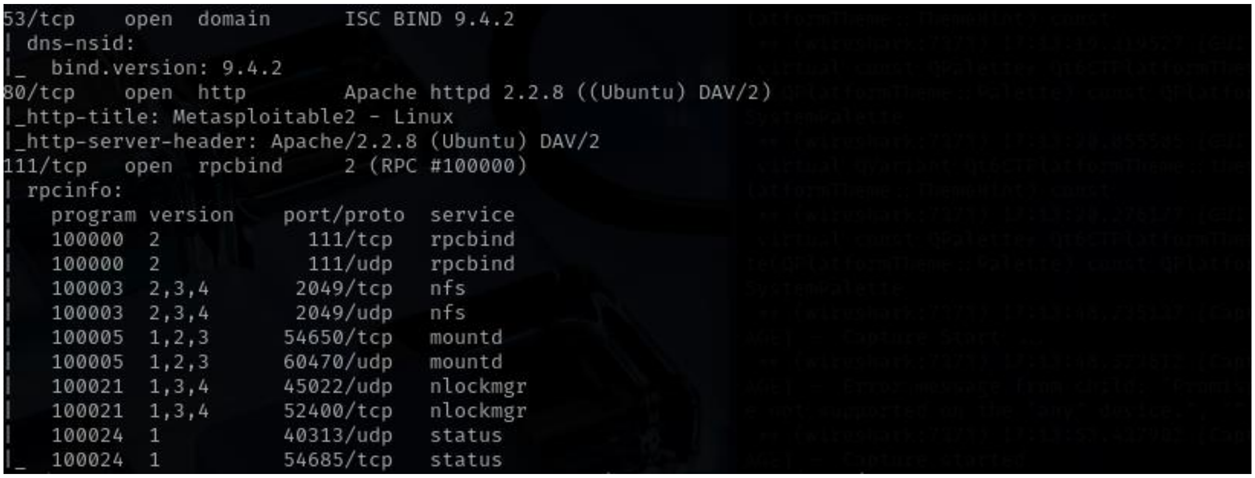


```
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
```

3. **Telnet (Port 23)**
   - **Service:** Linux telnetd
   - **Vulnerability:** Unencrypted transmission, prone to credential sniffing.
4. **SMTP (Port 25)**

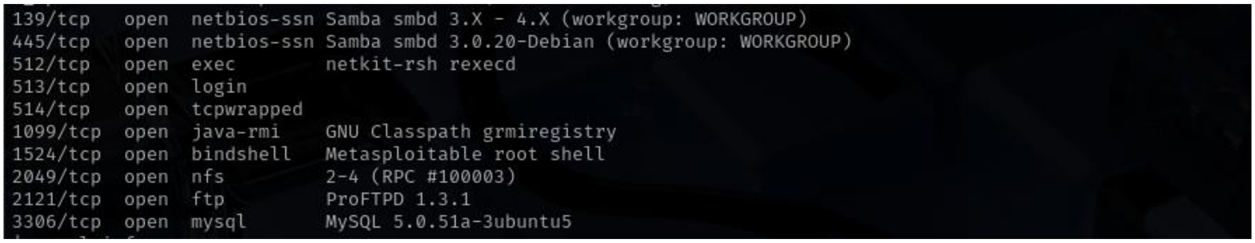
- **Service:** Postfix smtpd
- **STARTTLS Enabled:** Yes
- **Vulnerability:** Could allow enumeration of valid users through VRFY.

5. **DNS (Port 53)**
   - **Service:** ISC BIND 9.4.2
   - **Vulnerability:** Older version, may be susceptible to cache poisoning attacks.



```
53/tcp    open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      54650/tcp   mountd
|   100005  1,2,3      60470/udp   mountd
|   100021  1,3,4      45022/udp   nlockmgr
|   100021  1,3,4      52400/tcp   nlockmgr
|   100024  1          40313/udp   status
|_  100024  1          54685/tcp   status
```

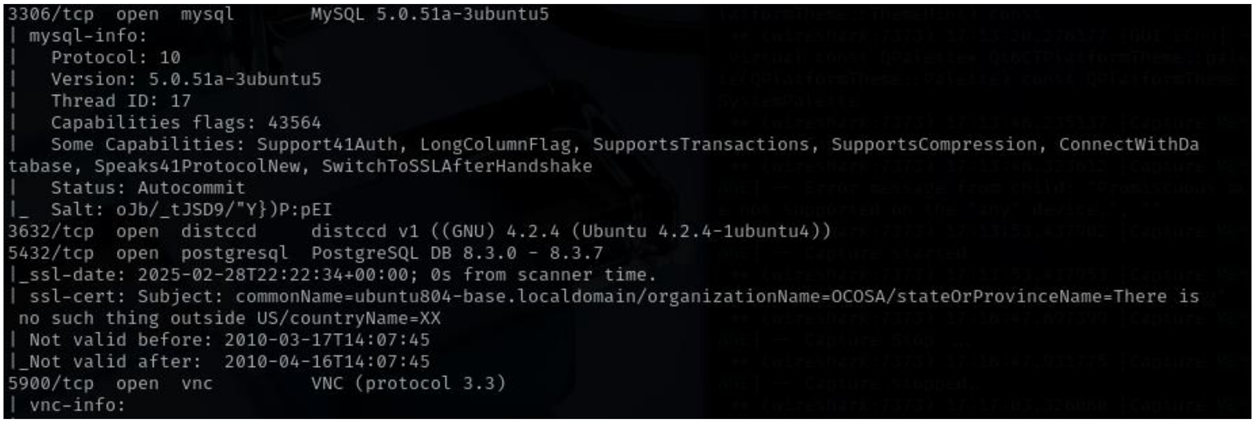
6. **HTTP (Port 80)**
   - **Service:** Apache 2.2.8 (Ubuntu)
   - **Vulnerability:** Version may be affected by several known exploits, including directory traversal and remote code execution.
7. **Samba (Ports 139 & 445)**
   - **Service:** Samba smbd 3.0.20-Debian
   - **Workgroup:** WORKGROUP
   - **Vulnerability:** Susceptible to SMB exploits such as EternalBlue.



```
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
```

8. **MySQL (Port 3306)**
   - **Service:** MySQL 5.0.51a-3ubuntu5

- **Vulnerability:** May be vulnerable to authentication bypass exploits.



```
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 17
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, LongColumnFlag, SupportsTransactions, SupportsCompression, ConnectWithDa
tabase, Speaks41ProtocolNew, SwitchToSSLAfterHandshake
|   Status: Autocommit
|_  Salt: oJb/_tJSD9/"Y})P:pEI
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-02-28T22:22:34+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
 no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
```

ka

9. **PostgreSQL (Port 5432)**
   - **Service:** PostgreSQL 8.3.0 - 8.3.7
   - **Vulnerability:** Older version, may be susceptible to SQL injection attacks.
10. **VNC (Port 5900)**
    - **Service:** VNC (protocol 3.3)
    - **Vulnerability:** If no password is set, attackers could gain unauthorized remote access.
11. **Apache Tomcat (Port 8180)**
    - **Service:** Apache Tomcat/Coyote JSP engine 1.1
    - **Vulnerability:** Tomcat default credentials might be used for unauthorized access.
12. **DistCC (Port 3632)**
    - **Service:** distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
    - **Vulnerability:** Open access can allow remote code execution (CVE-2004-2687).

Analysis & Recommendations:

1. **Disable anonymous FTP access** or upgrade vsftpd to a secure version.
2. **Upgrade OpenSSH to the latest version** to patch known vulnerabilities.
3. **Disable Telnet** and use SSH for secure remote access.
4. **Upgrade SMTP service** and restrict VRFY to prevent user enumeration.
5. **Upgrade BIND DNS** to the latest secure version to mitigate cache poisoning risks.
6. **Update Apache HTTP Server** to avoid known exploits.

7. **Harden Samba configuration** and ensure the latest security patches are applied.
8. **Upgrade MySQL and PostgreSQL** to mitigate SQL injection risks.
9. **Secure VNC with strong authentication** or disable it if not needed.
10. **Update Apache Tomcat** and remove default credentials.
11. **Disable or restrict distccd** to prevent remote code execution vulnerabilities.

Conclusion:

The target system is extremely susceptible, according to the scan, as it is using many out-of-date services that have known vulnerabilities. To protect the system from any threats, immediate security updates and mitigations are advised.